ABSTRACT

A certificate validity verification engine is integrated into the logic of a secure token, in turn, making the use of a private key conditional upon the determination that the certificate for the corresponding public key is valid at that particular instant in time. In this manner, the existence of a digital signature that is verified with a certificate implies that the certificate was valid at the time the signature was created. The verification of the certificate's validity by the relying party is unnecessary, as the signature could not have been created had the certificate been invalid. The validity of a certificate is communicated at the time the signature was created, rather than at the time the signature was verified.

0560569.00000